UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,396	02/18/2004	Sourabh Satish	SYMAP043	4350

21912 7590 10/10/2007

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
MEDE, ESTEVE	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
10/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,396	SATISH, SOURABH	
	Examiner	Art Unit	
	Esteve Mede	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18, and 29-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

1. This office action is responsive to application file on July 27, 2007. Claims 1-18 and 29-36 are pending. Claims 19-28 have been cancelled.

2. The 35 U.S.C. 112 second paragraphs rejection of claim 19 is withdrawn due to applicant's amendment.

3. The 35 U.S.C. 101 rejection of claims 1 37 and 38 is withdrawn due to applicant's amendment.

4. The objection of claims 1-18 and 29-36 is withdrawn due to applicant's amendment.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. **Claims 1-6, 18, 37-38** are rejected under 35 U.S.C. 102(e) as being anticipated by Schultz et al. (US 2003/0065926 A1).

Regarding claim 1 and 37-38, Schultz discloses a method for providing computer security comprising, providing an executable associated with a static state (para. 0021,lines 1-3); determining whether the executable meets a predetermined criterion (para. 0022, lines 3-9); associating a risk level with the executable, if it is

determined that the executable meets the predetermined criterion (para. 0038,lines 4-10); allowing the executable to execute if the first risk level does not exceed a threat level detection threshold (para. 0040), updating the first risk level to a second risk level that is higher than the first risk level if a process associated with the executable is observed to perform or attempt an action with which the second risk level is associated para. 0108); and performing a predetermined response action with respect to one or both of the process and the executable in the second risk level exceeds the threat detection threshold (para. 0022, and 0023); wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature (para. 0042, lines 9-14).

Regarding claim 2, Schultz discloses the method for providing computer security, wherein the risk level indicates a level of potential risk that will be brought by operating the executable (para. 0038, lines 3-6).

Regarding claim 3, Schultz discloses the method for providing computer security, wherein the risk level indicates how much risk the executable presents (para. 0099, lines 1-15; para. 0100, lines 1-3).

Regarding claim 3 Schultz discloses the method for providing computer security, wherein the risk level indicates a level of potential risk

Regarding claim 4, Schultz discloses the method for providing computer security, wherein the predetermined criterion includes a configuration criterion (para. 0036, lines 11-14; para. 0119, lines 8-18).

Regarding claim 5, Schultz discloses the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable is configured as a service (para. 0103, lines 3-4).

Regarding claim 6, Schultz discloses the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable is configured to run under a high privileged account (para. 0040, lines 4-8).

Regarding claim 18, Schultz discloses the method for providing computer security comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable (para. 0038, lines 4-8; para. 0099, lines 4-12).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 7-8, 10, 12-17, 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schultz et al. (US 2003/0065926 A1) in view of Tajalli et al. (US 2004/0143749 A1).

Regarding claim 7, Schultz discloses all the limitation of claim 7 as disclosed above in claim 1, except for wherein the predetermined criterion is used to determine whether the executable is installed via a standard procedure. The general concept of

whether the executable is installed via standard procedure is well known in the art as illustrated by Tajalli, which discloses controlling access to system resources by each process bases on a behavior control description for the process set to which it belongs (para. 0020, lines 5-7). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to in clued the use of a predetermined criterion to determine if the executable has not properly installed in order to prevent malicious code execution on a computer system, as well as to controlling access over malicious code.

Regarding claim 8, Schultz discloses all the limitation of claims 8 and 27 except, the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has sufficient access control. The general concept of determining if the executable having sufficient access control is well known in the art as illustrated by Tajalli, which discloses access control engine to monitor access and use of critical system resources, in addition the IDS watches applications request and resources used, looking for request or uses that depart from acceptable use and behavior (para. 0081, lines 1-11; para. 0161, lines 12-14; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining sufficient access control in order to control access rights to system resources.

Regarding claim 10, Schultz discloses all the limitation of claim 10, except the method of providing computer security, wherein the predetermined criterion is used to determine whether the executable is signed. The general concept of determining if the

executable is signed is well known in the art as illustrated by Tajalli, which disclose that the IDS will check for encryption within the executable (para. 0161, lines 12-14; para. 0169, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the executable is signed in order to determine the origin of the executable, as public key cryptography bind the signer to the key.

Regarding claim 12, Schultz discloses all the limitation of claim 12 and 26 except providing compute security wherein, the predetermined criterion includes a capability criterion. The general concept of the predetermined criterion includes a capability criterion is well known in the art as illustrated by Tajalli, which discloses the predetermined criterion include capability (para. 0055, lines 1-2; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of a capability criterion in order to protect the system against attack.

Regarding claim 13, Schultz discloses all the limitation of claim 13 and 28 except the method for providing computer security wherein the predetermined criterion is used to determine whether the executable has networking capability. The general concept of determining if the executable have network capability is well known in the art as disclosed by Tajalli, which discloses network protection against malicious codes (para. 0244, lines 1; 0251, lines 2-9; para. 0175, lines 5-6). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if malicious code has network capability in

order to protect the network against malicious codes that may cause damage to network.

Regarding claim 14, Schultz discloses all the limitation of claim 14 except, the method for providing computer security, wherein the predetermined criterion is used to monitor whether the executable has privilege manipulation capability. The general concept of determining whether the executable has privilege manipulation capability is well known in the art as illustrated by Tajalli, which discloses that the IDS would define modifying or manipulating registry keys as inappropriate behavior that would be blocked (para. 0050, lines 1-8). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if executable has privilege manipulation capability in order to protect the system against malicious codes that may want to modify system registries.

Regarding claim 15, Schultz discloses all the limitation of claim 15 except, the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has remote process capability. The general concept of determining if the executable has remote process capability is well known in the art as illustrated by Tajalli, which discloses the IDS is configured to control network services to include remote connection (para. 0236, lines 1-3; para. 0239, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if malicious code has remote capability in order to prevent the network from being taking over by hackers that may use Trojan Horses to enter the network unchecked.

Regarding claim 16, Schultz discloses all the limitation of claim 16 except, the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has process launching capability. The general concept of determining if the malicious code has process launching capability is well known in the art as illustrated by Tajalli, which discloses a malicious code initiate HTTP connection to other Web servers (para. 0244, lines 1-2; para. 0249, lines 1-2). Therefore it would have been obvious for one ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the malicious code has process launching capability in order to stop malicious code from executing and from calling other system resources from the network.

Regarding claim 17, Schultz discloses all the limitation of claim 17 except, the method for providing computer security, wherein the predetermined criterion is used to determine whether the executable has secure algorithm. The general concept of determining if malicious codes has secure algorithm is well known in the at as illustrated by Tajalli, which discloses the IDS controls access to any attributes of files or directories including if encryption present for the malicious code (para. 0217, lines 1-2; para. 0222, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of determining if the malicious code has secure algorithm in order to protect against virus that uses encrypted code to hide their payload from virus protection mechanism.

Regarding claim 29-31, Schultz discloses all the limitation of claim 29-31 as disclosed above except, the method for providing computer security, comprising

analyzing historical evidence; the historical evidence include a record of activities and log file. The general concept of analyzing historical evidence is well known in the art as illustrated by Tajalli, which discloses the use of historical evidence (para. 0091, lines 1-7; para 0097, line 1). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of analyzing historical evidence, record activities and log file in order to assign processes into their proper category, thus that new policy may be implemented more effectively.

Regarding claim 32, Schultz and Tajalli disclose all the limitation of claim 32 as disclosed above except, the method for providing computer security, wherein the historical evidence includes a system optimization file. The general concept of the historical includes a system optimization file is well known in the art by Tajalli, which disclose a communication module to retrieve configuration or log data and returns them, in addition the communication module can retrieve data from disk or from the engine, and request alert when unusual event occur (para 0090, lines 3-8). System optimization file or swap files resides on disk. Therefore it would have been obvious for one of ordinary skill in that art at the time of the invention to modify Schultz to include the use of swap file in order to obtain information that are relevant to build system policy.

Regarding claim 33-34, Schultz discloses all the limitation of claim 33 and 34 as disclosed above except the method for providing computer security, wherein historical evidence includes a crash dump. The general concept of the historical evidence includes a crash dump is well known in the art as illustrated by Tajalli, which discloses a communication module that monitors local log files, transfers log data to a management

infrastructure and request alerts when unusual events occur (para. 0090, lines 3-8). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use a crash dump file and prefetch file in order to gather information when system failure occur.

10. **Claims 9, 11, 35-36** are rejected under 35 U.S.C. 103(a) as being unpatentable over Schultz et al. (US 2003/0065926 A1) in view of Khazan et al. (US 2005/0108562 A1).

Regarding claims 9, and 11, Schultz discloses all the limitation of claim 9 and 11 except the method of providing computer security, wherein the predetermined criterion is used to determine whether the executable is recent and determine whether the executable has a modified date different from the created date. The general concept of determining whether the executable is recent and determining whether the executable has a modified date different from the created date is well known in the art as illustrated by Khazan, which discloses analyzing the executable when modification take place (para. 0107, lines 1-4; para. 0115, lines 1-19). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of Khazan in order to verify whether modification has taken place within the executable.

Regarding claims 35-36, Schultz discloses all the limitation of claim 35 except, the method for providing computer security, comprising performing a dynamic risk analysis, and determining whether an action is required. The general concept of

performing dynamic analysis and determining whether an action is required is well known in the art as illustrated by Khazan, which discloses static and dynamic analyzer (para. 0040, lines 12-13, and whether an action is required (para. 0099, lines 7-11, lines 21-26). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Schultz to include the use of dynamic analyzer to determine whether an action is required in order to protect compute systems against malicious codes.

Response to Arguments

12. Applicant's arguments filed 07/21/207 have been fully considered but they are not persuasive.

Applicant basically argues that Schultz a static analysis. Examiner disagrees Schultz discloses two risk level based a predetermined threshold. Further Schultz discloses another risk level (borderline), which updates periodically and is able to generate new detection models if a predetermined threshold is exceeded and distribute the updated model to the malicious content detector (para. 0107-0108). Therefore the invention of closes is not solely a static detector as it may also increase the risk level from borderline to malicious.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede

EM
September 28,2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER